10621731

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00

A1

(11) International Publication Number: **WO 00/65426**

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/US00/08536

(22) International Filing Date: 29 March 2000 (29.03.00)

(30) Priority Data:
09/298,360 23 April 1999 (23.04.99) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

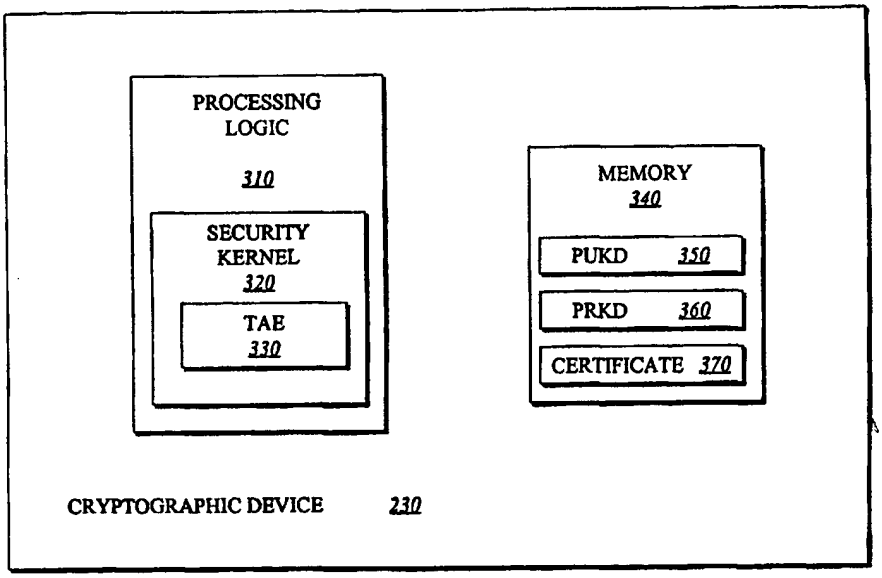
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DAVIS, Derek, L. [US/US]; 4509 East Desert Trumpet Road, Phoenix, AZ 85044 (US). HERBERT, Howard, C. [US/US]; 16817 South 1st Drive, Phoenix, AZ 85045 (US).

(74) Agents: MILLIKEN, Darren, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: CRYPTOGRAPHIC DEVICE AND METHOD FOR ASSURING INTEGRITY OF TRUSTED AGENT COMMUNICATIONS



(57) Abstract

A cryptographic device comprising a processing logic and memory associated with the processing logic. The memory is loaded with a first segment of code to control execution of cryptographic functions and hash functions, and a second segment of code to perform cryptographic functions on behalf of a third party having no physical control of hardware employing the cryptographic device.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CRYPTOGRAPHIC DEVICE AND METHOD FOR ASSURING INTEGRITY OF TRUSTED AGENT COMMUNICATIONS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of cryptography. In particular, this invention relates to a system and method to protect digital content resident in a digital platform.

2. General Background

For many years, there has been a growing demand for platforms that provide video programming for entertainment purposes. Normally, the video programming (e.g., pay-per-view movies) is transmitted in an analog format such as National Television Systems Committee (NTSC) or Phase Alternating Line (PAL). Due to the inherent nature of analog signaling, video programming is protected because recorded copies normally would have poorer image quality than the original master. Also, copy protection signals may be added to the signaling in order to prevent its successful recordation. The inherent nature of content in a digital format, however, fails to provide these safeguards against modification and recordation.

Currently, original equipment manufacturers (OEMs) are developing open, re-programmable digital platforms to receive content in a digital format. For example, in the case of pay-per-view movies, a customer issues a request to a content provider (e.g., a cable company) to download a movie to the digital platform. Upon receiving authorization, the movie is downloaded and, in accordance with one purchasing scheme, an appropriate charge is debited from a prepaid balance maintained by the digital platform. This purchasing scheme is referred to as "metered content." When the prepaid balance has been exhausted, the customer initiates contact with the content provider or an independent third-party source to establish additional credit.

Unfortunately, since many digital platforms are open and programmable, their functional elements (e.g., hardware, software, or firmware) can be observed and modified by an unauthorized user or by a malicious program. As a result, it is difficult for content providers to ensure that a digital platform is operating as intended. Encrypting the communication channels or using conventional digital signatures may prevent content from being unknowingly modified during transmission; however, these techniques do not provide assurances to the content provider that the content, once loaded within the digital platform, has not been illicitly modified. For example, there is no protection against disabling content metering software responsible for debiting the prepaid balance or modifying content metering software responsible for crediting the prepaid balance.

Moreover, even if the software has not been corrupted, there are no assurances to the content provider that communication or processing circuitry within the digital platform has not been compromised. For example, substitute circuitry or software (e.g., motherboard circuitry, basic input/output system "BIOS", operating systems, etc.) may be deployed within the digital platform which does not comply with the desired content metering scheme. Additionally, hardware-based methods, such as use of a logic analyzer , may compromise the scheme. These security threats have greatly impeded the expansion of digital content distribution.

Therefore, it is desirable to provide a digital platform and protocol to ensure that the digital platform and its implemented functional elements are authorized and are operating as intended.

SUMMARY OF THE INVENTION

A cryptographic device comprising a processing logic and memory associated with the processing logic. The memory is loaded with a first segment of code to control execution of cryptographic functions and hash functions, and a second segment of code to perform operations on behalf of a third party having no physical control of hardware employing the cryptographic device.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an illustrative block diagram of an embodiment of a system to transfer content from a head-end to a digital format.

Figure 2 is an illustrative block diagram of an embodiment of the digital platform of Figure 1.

Figure 3 is an illustrative block diagram of a cryptographic device associated with the digital platform.

Figure 4 is an illustrated embodiment of the protocol followed by the TAE and security kernel to configure the system of Figure 1.

Figure 5 is an illustrative embodiment of the protocol followed by the GUI and head-end equipment to configure the system of Figure 1.

Figure 6 is an illustrative embodiment of the validation of the device certificate chain.

Figure 7 is an illustrative embodiment of the operations for recovering the combined result, inclusive of TAEH and MH, from the notary digital signature.

Figure 8 is an illustrative block diagram of an embodiment of the present invention in which the recovered TAEH and computed TAEH are compared.

Figure 9 is an illustrative block diagram of an embodiment of the present invention in which the recovered MH and computed MH are compared.

Figure 10 is an illustrative block diagram of an embodiment of a billing procedure conducted by the digital platform after system configuration.

DETAILED DESCRIPTION

The present invention relates to a system and a corresponding method for ensuring that a programmable digital platform is operating as intended. This is accomplished by providing a protocol that enhances protection of the integrity of data transferred to the digital platform. While certain details are set forth in order to provide a thorough understanding of the present invention, it should be appreciated that these details should not limit the scope or applicability of the present invention. Likewise, well-known circuitry is not discussed in great detail to avoid unnecessarily obscuring the present invention.

In the following description, some terminology is used to describe certain characteristics of the present invention as well as cryptographic functionality. For example, "content" is generally defined as (i) control information (e.g., Internet Protocol "IP" commands, keys, digital signatures, digital certificates, etc.), and/or (ii) data in the form of a still image, video (e.g., a movie, television programming, pay-per-view programming, a video game, etc.), audio, software and the like. A "channel" is generally defined as a pathway through which content may be transferred over one or more information-carrying mediums such as, for example, electrical wire, fiber optic, cable, bus trace, plain old telephone system (POTS) line, wireless (e.g., satellite, radio frequency "RF", infrared, etc.) or even a logical link.

With respect to cryptographic functionality, a "key" is information used by a cryptographic function to perform a particular operation related to encryption or decryption. A "cryptographic function" is a software routine or a collective acts related to encryption, decryption and/or digital signaturing. Examples of cryptographic functions include a symmetric key cryptographic function (e.g., Data Encryption Standard "DES"), an asymmetric (public key) cryptographic function (e.g., Rivest, Shamir and Adleman "RSA" based functions), or even a function for digitally signing information (e.g., Digital Signature Algorithm "DSA" or a RSA-based signing functions).

In addition, a "digital certificate" is generally defined as any information used for authentication. Normally, this information includes a public key encrypted with a private key of a certification authority (PRKCA). A "certification authority" includes any person or entity in a position of trust to guarantee or sponsor the digital certificate. A "digital signature" is generally used to ensure that the data has not been illicitly modified after being digitally signed. The data may be provided in its entirety, or as a hash value produced by a hash function. A "hash function" involves an operation where content of a variable-length is converted into a fixed-length hash value. Normally, hash functions are "one-way" so that there does not readily exist an inverse function to recover a portion of the original content from the hash value. Examples of a hash function include MD2 or MD5 provided by RSA Data Security of Redwood City, California, or Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology located in Washington, D.C.

Referring to Figure 1, a perspective view of an illustrative embodiment of a system utilizing the present invention is shown. In this embodiment, system 100 includes head-end content distribution equipment 110 that is controlled by a content provider. Normally, head-end equipment 110 is remotely located from and in communication with a digital platform 130 through a channel 120. An example of head-end equipment 110 includes, but is not limited or restricted to a satellite, a cable station, or any hardware capable of downloading content. The content may be in real-time or prestored on a hard disk drive, a compact disk, a digital video disk, a digital tape or any other type of medium. Of course, it is contemplated that the present invention may also ensure that the integrity of communications between digital platform 130 and a peripheral or other content storage device is maintained.

Referring now to Figure 2, an illustrative block diagram of digital platform 130 is shown. Digital platform 130 comprises a casing 200 protecting a substrate 210 contained therein. Substrate 210 is formed from any type of material or combination of materials upon which integrated circuit (IC) devices can be attached such as memory 220 and a cryptographic device 230. Substrate 210 may be produced in a number of form factors such as, for example, a circuit board acting as a motherboard or a removable

daughter card, a network interface card (NIC), and the like. Digital platform 130 receives input from one or more input peripherals 240 (e.g., a mouse, keyboard, infrared controller, etc.) and produces an output, perceived by the user, on an output device 250 (e.g., a display monitor, speakers, etc.).

In this embodiment, memory 220 includes software that, when executed, operates as a graphical user interface (GUI). It is contemplated that memory 220 may further include content usually in an encrypted digital format if communications between memory 220 and cryptographic device 230 are secure and/or memory 220 itself is secure. For example, memory 220 can constitute secure storage when it is generally infeasible for an unauthorized individual to successfully access content from memory 220 in an non-encrypted format and/or tamper with the data without detection. Different security mechanisms include packages designed to destroy information on ICs when tampered, and tamper resistant software as described in U.S. patent application entitled "Tamper Resistant Methods and Apparatus", Application No. 08/662/679, filed June 13, 1996 which has issued as U.S. Patent No. _____. Of course, there exist many other embodiments of security mechanisms that differ in design but do not deviate from the spirit and scope of the invention.

Herein, cryptographic device 230 is implemented as a coprocessor operating in coordination with a host processor. However, it is contemplated that cryptographic device may be implemented within a chipset, or implemented as the host microprocessor, a controller, or any other electronic device having data processing capability.

Referring now to Figure 3, in this embodiment, cryptographic device 230 comprises processing logic 310 having a limited amount of memory loaded with a first segment of code 320 and a second segment of code 330. The first segment 320, referred to as a "security kernel," includes code that, when executed, controls the operations of code 330 and controls the execution of cryptographic functions, hash functions and other generate management functions used to protect the integrity of data provided to the content provider. In this embodiment, security kernel 320 is running at Ring 0 of device 230 although it is not required. The security kernel 320 is generally a permanent element of device 230, loaded therein at manufacture and subject to unauthorized removal or

modification. The second segment of code 330 is referred to as a "trusted agent executable (TAE)." When executed, TAE 330 performs operations on behalf of a third party having no physical control of the digital platform. This code supports content metering as well as other functionality. Also, TAE 330 operates in combination with security kernel 320 to produce a data packet for transmission to head-end equipment 110 of Figure 1. This data packet provides information to the content provider to determine that the originator of the data packet was indeed TAE 330 and that the integrity of communications between the content provider and TAE 330 is protected. TAE 330 is loaded on an "as needed" basis in the field. Different TAEs, provided by multiple, independent third parties may exist and be loaded at various times into device 230.

As further shown, cryptographic device 230 also comprises internal memory 340 loaded with a device public key (PUKD) 350, a device private key (PRKD) 360 and device certificate chain 370, all data uniquely associated with cryptographic device 230. In particular, to permanently retain its stored data, memory 340 may be implemented as non-volatile memory (e.g., read only memory, any type of programmable read only memory, flash memory, etc.) or volatile memory (e.g., random access memory "RAM", battery backed RAM, etc.). As an alternative embodiment, however, memory 340 may also include security kernel 320 and TAE 330 in the event of memory space constraints.

As further shown, device certificate chain 370 includes one or more "device certificates" which are data used to identify cryptographic device 230. For example, certificate 370 includes PUKD 350 digitally signed with PRKCA. Herein, PRKCA is a private key of a manufacturer of cryptographic device 230. However, it is contemplated that PRKCA may be a private key of another certification authority such as, a bank, governmental entity, trade association, or other original equipment manufacturer.

Referring now to Figure 4, an embodiment of a protocol used to configure the system is described. This protocol is designed to protect the integrity of content received from a trusted agent executable (TAE) employed within the digital platform. During configuration, a graphical user interface (GUI) is installed within the digital platform (block 400) while a selected type or version of TAE is loaded into memory of the cryptographic device of Figure 2 (block 405). Thereafter, in block 410, the security

kernel of the cryptographic device computes a hash value for the TAE (referred to as a trusted agent executable hash "TAEH"). This is accomplished by a single or iterative hash operations on the TAE. TAEH is temporarily stored within secure memory of the cryptographic device (block 415), accessible to the security kernel but not to the TAE.

After producing TAEH, the cryptographic device commences execution of the TAE. As one possible activity, the TAE produces a request for generation of a key pair by the security kernel (block 420). This key pair includes a pair of unique public and private keys (PUKTAE and PRKTAE) to be associated with this specific instantiation of this type or version of the TAE. Upon receipt, the key pair is stored in secure memory (block 425), accessible to the TAE. In one embodiment, PUKTAE is included within a message to (i) identify the TAE, (ii) enable verification of the integrity of data produced by the digital platform, and (iii) enable confidential communications with the TAE. This message (M) may include, for example, a copy of data provided to the head-end equipment and/or a current monotonic count value. Message (M) undergoes a hash operation to produce a message hash (MH) prior to submission to the security kernel (block 430). Of course, as alternative embodiments, the hash operation may be performed by the security kernel instead of at the application level.

Thereafter, the cryptographic device initiates an internal call for the security kernel (block 435) to perform a "digital notarization" of MH, which is then executed by the kernel in blocks 440-450. In block 440, the MH provided by the TAE is combined with the previously stored TAEH and possibly with an "assertion", e.g. by concatenation, modulo addition or any another arithmetic operation. The "assertion" is a statement indicating the purpose for a digital signature. For example, the assertion may include information concerning the type, model or version number of the cryptographic device. By combining the kernel-produced TAEH with at least MH, the digital notarization allows the content provider to detect if MH has been produced by a modified TAE. After TAEH, MH and perhaps the assertion are combined (block 440), the combined result is digitally signed with PRKD to produce a "notary digital signature" (NDS) as shown in block 445. NDS along with a device certificate chain, namely at least one certificate including PUKD encrypted with PRKCA, is returned to the TAE (block 450).

Additionally, the TAEH, assertion, and combined result from block 440 may be returned to the TAE in the event that these values are not predeterminable.

As shown in Figure 5, upon receipt of NDS, the device certificate chain and other optional information, TAE passes the same to the GUI of the digital platform (block 500). The GUI is designed to contact the head-end equipment and to upload this information to the head-end equipment (block 505).

At the head-end equipment, the device certificate chain is validated to recover data, inclusive of PUKD as also shown in Figure 6 where "D" constitutes a digital signature verify function (block 510). Since the notary digital signature has been digitally signed by PRKD, the recovery of PUKD allows the message hash, TAEH and perhaps the assertion to be recovered and validated as shown in Figure 7 (block 515). Since the content provider created the original TAE, the TAE as known to be correct by the head-end equipment may be configured to undergo a hash operation (using the same one-way hash function as used by the cryptographic device) to produce a computed TAEH (referred to as "$TAEH_c$") as shown in Figure 8 (block 520). Such $TAEH_c$ would normally to precomputed and stored at the head-end equipment. $TAEH_c$ is compared to the recovered TAEH (block 525). If the comparison is successful, the head-end equipment is assured that no illicit modification of the TAE has occurred. Otherwise, an error condition is reported and the head-end equipment may take appropriate action (e.g., ignore the communication, send an "alert" to the client GUI, etc.) as shown in block 530.

Similarly, to verify the integrity of the data and check that the message originated from an authorized cryptographic device, the message (M) undergoes a hash operation to compute a resultant message hash (MH_c) as set forth in block 535 and shown in Figure 9. MH_c is compared to the recovered MH (block 540). If the comparison is successful, the head-end equipment is assured that message (M) has not been modified during transmission. Otherwise, the head-end equipment may take appropriate action (block 545).

After the comparisons have been performed and each comparison deemed successful, one or more keys needed to decrypt portions of preloaded, encrypted digital

information (referred to as "content keys") may be provided to the GUI and directed to the TAE of the cryptographic device via channel 120 of Figure 1 (block 550). In particular, the content keys are encrypted with PUKTAE that was provided within the message M and is now available to the content provider. The content keys are provided to and stored internally within secure memory of the cryptographic device to mitigate the chances of uncovering the content keys in a plain text format (block 555). Of course, in lieu of storing the content decryption keys within the cryptographic device, it is contemplated that the protocol may be performed every time after power-up so no permanent content key storage is necessary.

After configuration of the cryptographic device, occasional communications between the digital platform and the content provider may occur for a number of purposes, including credit establishment for example. During these communications, it can be determined whether the digital platform is operating properly or is authorized to receive content keys to decrypt portions of digital content stored in internal memory of the digital platform by cryptographic device providing M, NDS and the device certificate.

Referring now to Figure 10, an illustrative embodiment of a billing procedure conducted by the cryptographic device after installation of TAE is shown. First, in block 600, a prepaid balance is maintained in secure memory associated with the cryptographic device. This prevents the prepaid balance from being modified. Through GUI software, the consumer is provided a listing of prestored encrypted content such as movies, video games and the like (block 610). Upon the consumer selecting a particular portion of the encrypted content, the GUI passes a message to the TAE indicating that the user has authorized the purchase or limited usage of that particular portion of the encrypted content (block 620). Also, the portion of encrypted content may be routed to the TAE. In response, the TAE determines if the prepaid balance covers the cost of the selected content (block 630). Note that block 650 may be initiated by the user to increase the prepaid balance without the explicit attempt to purchase content.

In the event the prepaid balance is less than the cost of the selected content, a function call may occur to produce a message on a display indicating to the user that the

outstanding balance is insufficient to purchase the content (block 640). After perceiving the message, the user activates the GUI to contact the head-end equipment and provides, if not previously provided, credit card information, automated teller machine (ATM), checking account routing number or any other financial information to the head-end equipment (block 650) in order to increase the outstanding balance by a selected amount. The head-end equipment and the TAE mutually authenticate each other to ensure that their communication path is secure as described in Figures 4 and 5 (block 660). This protects the system against anti-replay conditions. Once the communication path is secure and authorization for a financial debit is received, the head-end equipment transmits a message to the TAE to increase the prepaid balance by the selected amount (block 670). The TAE adds the selected amount to the outstanding balance in secure memory (block 680).

If the prepaid balance then or now exceeds the cost of the selected content, the TAE decrements the outstanding balance by the appropriate costs of the selected content (block 690). Thereafter, a key previously loaded into secure memory of the processing logic is used to decrement the encrypted content (block 700). The plain text version of the content is returned to the GUI for installation on the digital platform for later viewing, listening or other sensory perception by the user (block 710).

The present invention described herein may be designed in accordance with many different methods and using many other embodiments that may come to mind to a person skilled in the art, without that person departing from the spirit and scope of the present invention. The invention should, therefore, be measured in terms of the claims which follow.

CLAIMS

What is claimed is:

1. A cryptographic device comprising:

a processing logic; and

a memory associated with the processing logic, the memory loaded with (i) a first segment of code to control execution of cryptographic functions and hash functions, and (ii) a second segment of code to perform operations on behalf of a third party having no physical control of hardware employing the cryptographic device.

2. The cryptographic device of claim 1 further comprising the memory further includes a public key of the cryptographic device, a private key of the cryptographic device and a digital certificate chain including at least one device certificate.

3. The cryptographic device of claim 2, wherein the memory includes an on-chip memory situated on a chip with the processing logic and an off-chip memory.

4. The cryptographic device of claim 3 further comprising a package containing the off-chip memory, the processing logic and the on-chip memory.

5. The cryptographic device of claim 1, wherein the first segment of code is running at ring 0.

6. The cryptographic device of claim 2, wherein the first segment of code produces a notary digital signature including a combined result of a hash value of a message and a hash value of the second segment of code, the combined result digitally signed by the private key of the cryptographic device.

7. The cryptographic device of claim 6, wherein the combined result further includes an assertion indicating a purpose of the notary digital signature.

8. The cryptographic device of claim 7, wherein the hash value of the message, the hash value of the second segment of code and the assertion are concatenated to produce the combined result.

9. The cryptographic device of claim 7, wherein the hash value of the message, the hash value of the second segment of code and the assertion undergo modular addition to produce the combined result.

10. The cryptographic device of claim 6, wherein the second segment of code passes the message, the notary digital signature and the digital certificate chain to a graphical user interface.

11. A digital platform comprising:

a substrate;

a memory coupled to the substrate, the memory including a graphical user interface and content in an encrypted format; and

a cryptographic device coupled to the substrate and in secure communications with the memory, the cryptographic device being loaded with a trusted agent executable to (i) perform content metering on behalf of an entity having no physical control of the digital platform, and (ii) preserve the integrity of data transmitted from and received by the digital platform.

12. The digital platform of claim 11, wherein the cryptographic device further comprises a security kernel being code, in communications with the trusted agent executable, that produces a notary digital signature including a combined result of at least a hash value of a message and a hash value of the trusted agent executable digitally signed by a private key of the cryptographic device.

13. The digital platform of claim 12, wherein the combined result associated with the notary digital signature further includes an assertion indicating a purpose of the notary digital signature.

14. The digital platform of claim 13, wherein the hash value of the message, the hash value of the trusted agent executable and the assertion are concatenated to produce the combined result.

15. The digital platform of claim 12, wherein the memory is provided with a content key from a remote source after transmission of the combined result.

16. A method for ensuring the integrity of data exchanged between a platform and a remotely located content provider, comprising:

receiving a selected trusted agent executable by the platform; and

providing a notary digital signature to the content provider, the notary digital signature including a combined result of a hash value of a message and a hash value of the selected trusted agent executable, the combined result digitally signed by a private key associated with the cryptographic device.

17. The method of claim 16, wherein the combined result of the notary digital signature further includes an assertion to indicate a purpose of the notary digital signature.

18. The method of claim 17 further comprising:

providing the message and a device certificate chain to the content provider, the device certificate chain including at least one device certificate having a key associated with the platform for use in recovering the hash value of the message, the hash value of the selected trusted agent executable and the assertion from the notary digital signature.

19. The method of claim 18 further comprising:

performing a hash operation on a copy of a selected trusted agent executable as provided to the digital platform by the content provider;

comparing a hash value associated with the copy of the selected trusted agent executable with the recovered hash value of the trusted agent executable; and

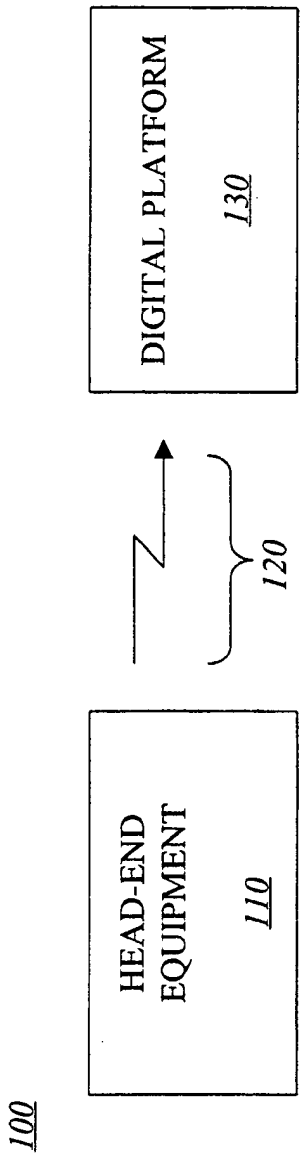
confirming that the trusted agent executable at the platform has not been modified upon successful comparison between the copy of the selected trusted agent executable and the recovered hash value of the trusted agent executable.

20. A machine readable medium having embodied thereon code for processing by a platform including memory containing the code, comprising:

a trusted agent executable to perform content metering operations on behalf of an entity or person without physical control of the platform; and

a security kernel in communication with the trusted agent executable, the security kernel to generate a notary digital signature including a hash function of the trusted agent executable and an assertion being data to indicate a purpose of the notary digital signature.

Figure 1



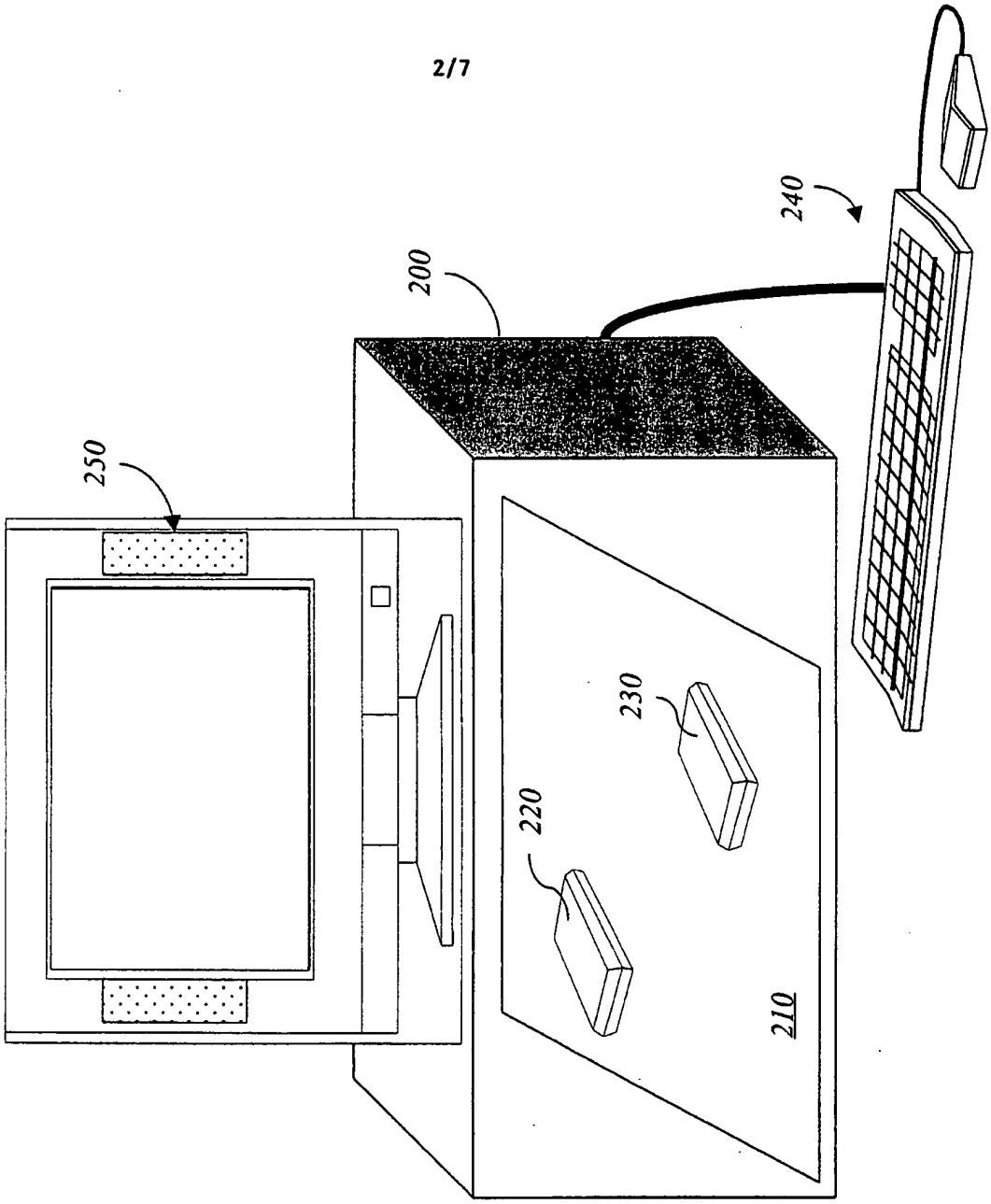


Figure 2

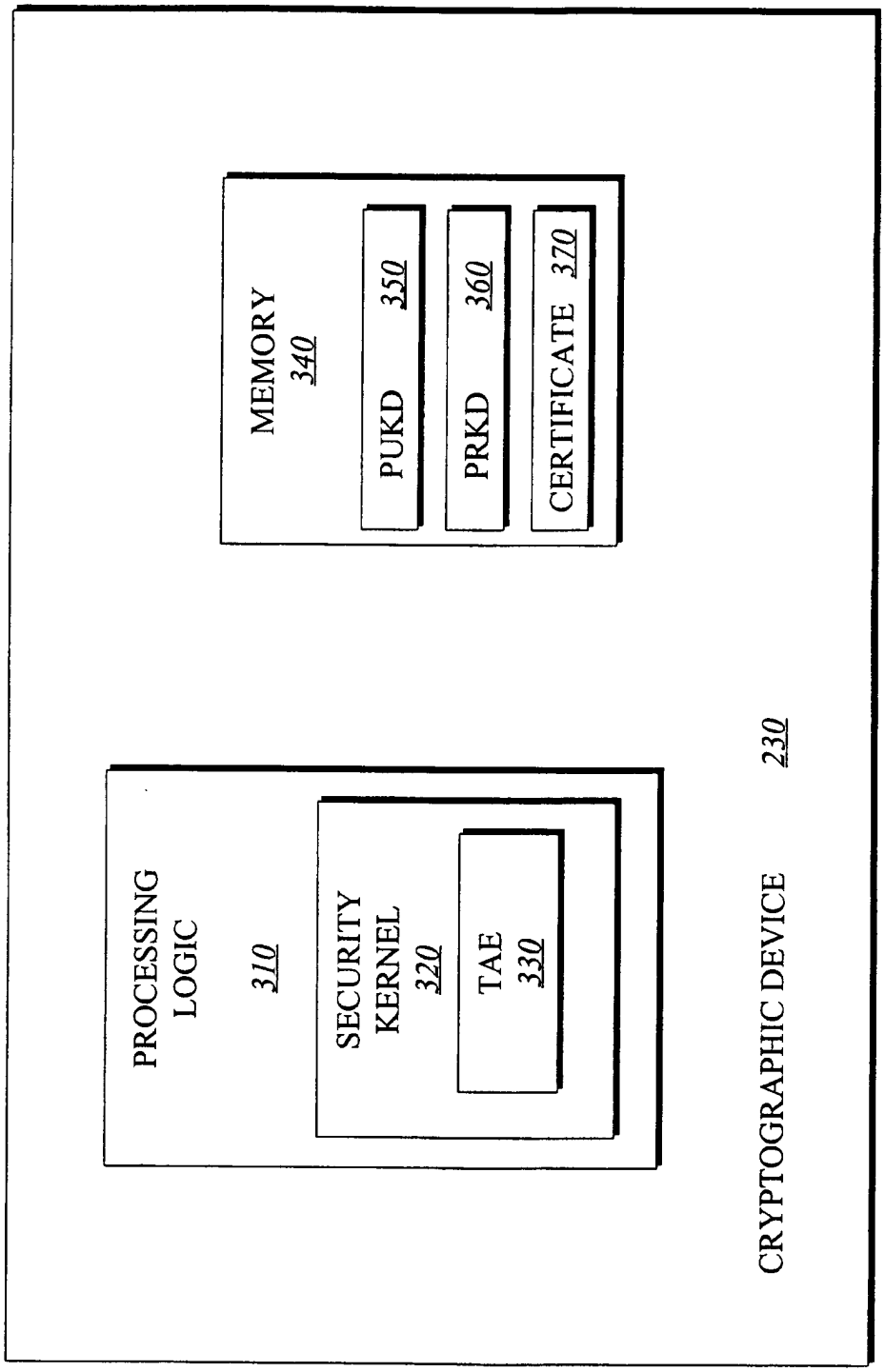
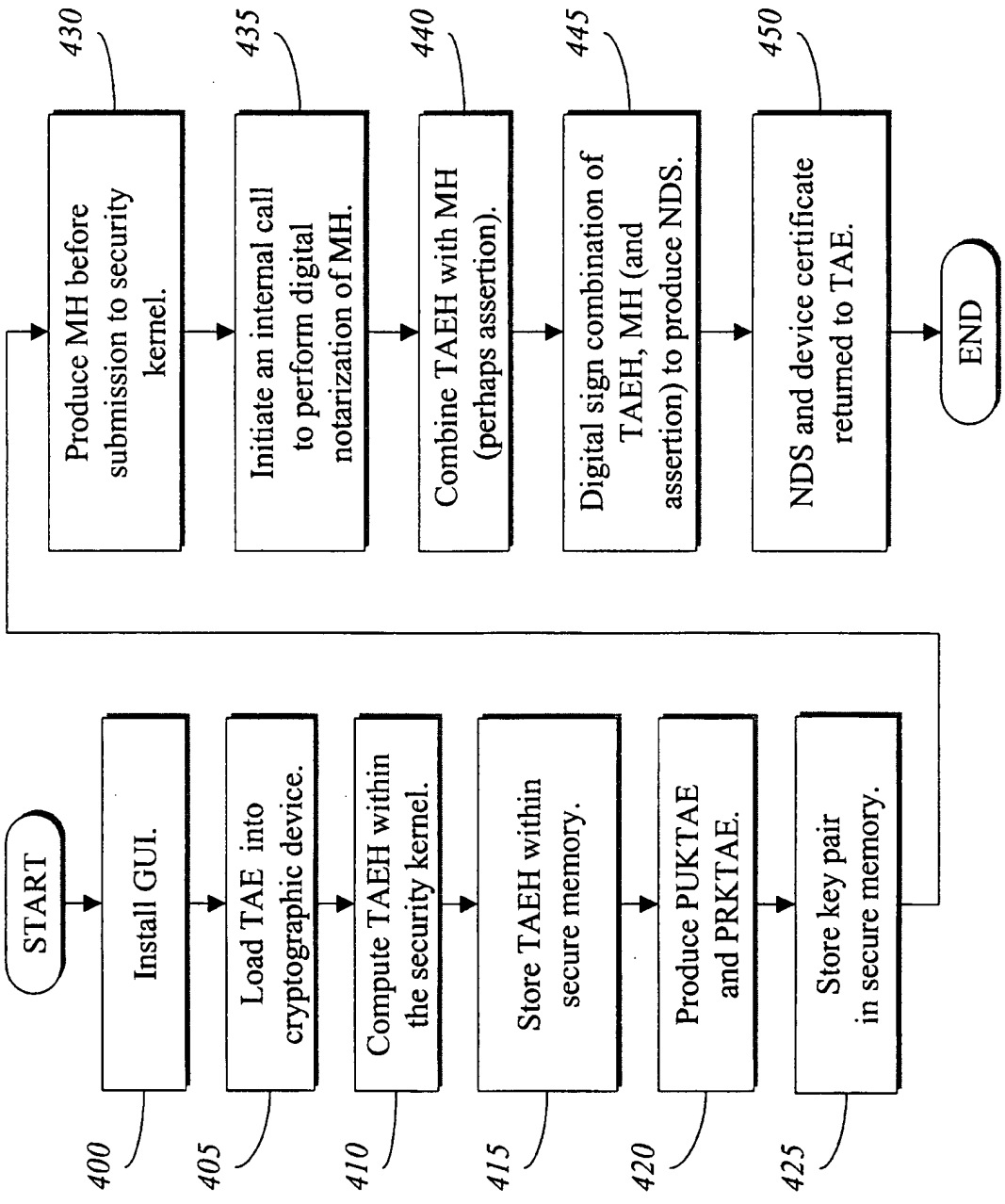

CRYPTOGRAPHIC DEVICE 230
PROCESSING LOGIC 310
SECURITY KERNEL 320
TAE 330
MEMORY 340
PUKD 350
PRKD 360
CERTIFICATE 370

Figure 3

Figure 4


START
Install GUI.
Load TAE into cryptographic device.
Compute TAEH within the security kernel.
Store TAEH within secure memory.
Produce PUKTAE and PRKTAE.
Store key pair in secure memory.
Produce MH before submission to security kernel.
Initiate an internal call to perform digital notarization of MH.
Combine TAEH with MH (perhaps assertion).
Digital sign combination of TAEH, MH (and assertion) to produce NDS.
NDS and device certificate returned to TAE.
END
400
405
410
415
420
425
430
435
440
445
450

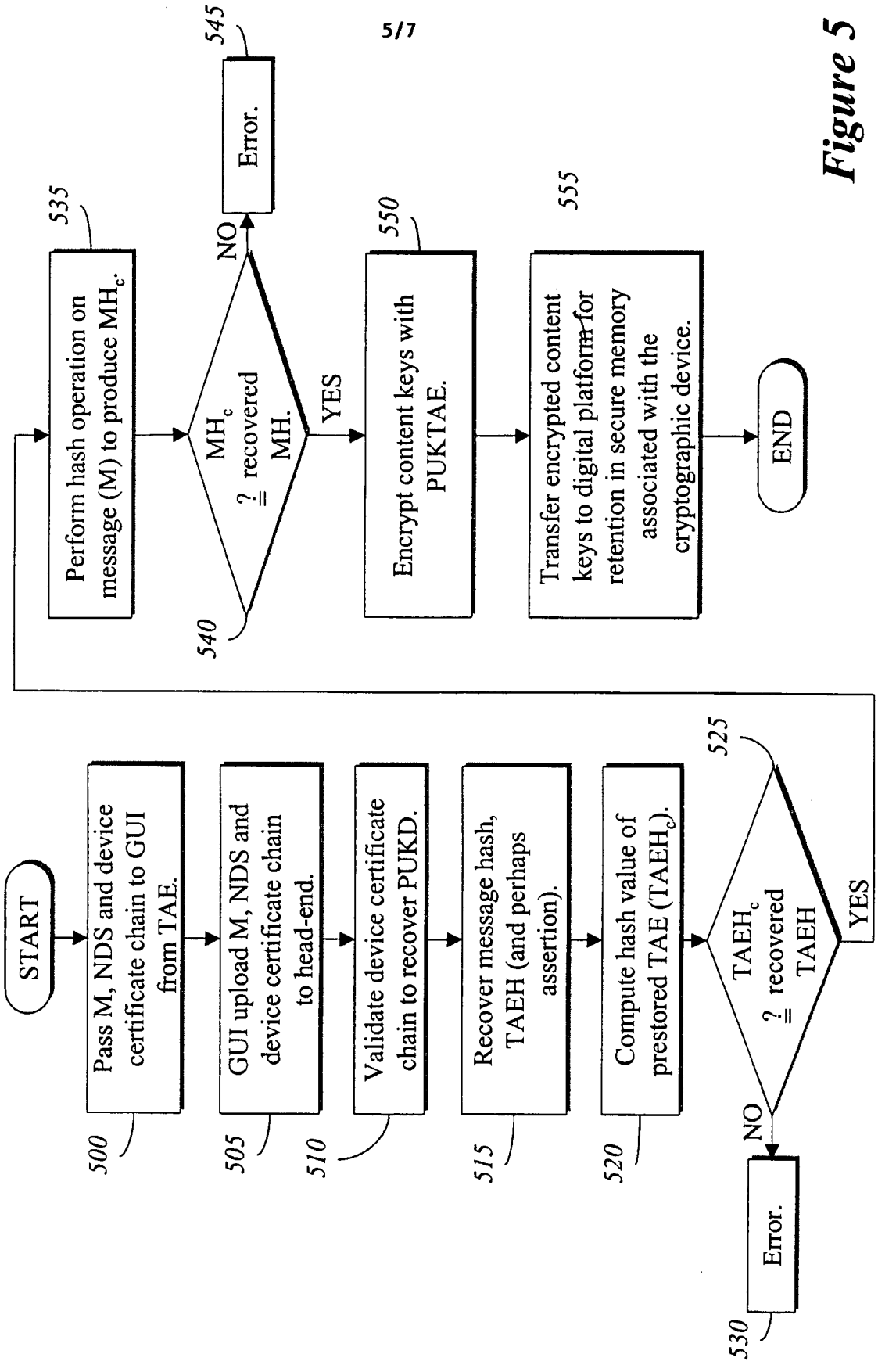

START
Pass M, NDS and device certificate chain to GUI from TAE.
GUI upload M, NDS and device certificate chain to head-end.
Validate device certificate chain to recover PUKD.
Recover message hash, TAEH (and perhaps assertion).
Compute hash value of prestored TAE (TAEH$_c$).
TAEH$_c$? ≡ recovered TAEH
NO
YES
Error.
Perform hash operation on message (M) to produce MH$_c$.
MH$_c$? ≡ recovered MH.
NO
YES
Error.
Encrypt content keys with PUKTAE.
Transfer encrypted content keys to digital platform for retention in secure memory associated with the cryptographic device.
END
500
505
510
515
520
525
530
535
540
545
550
555

Figure 5

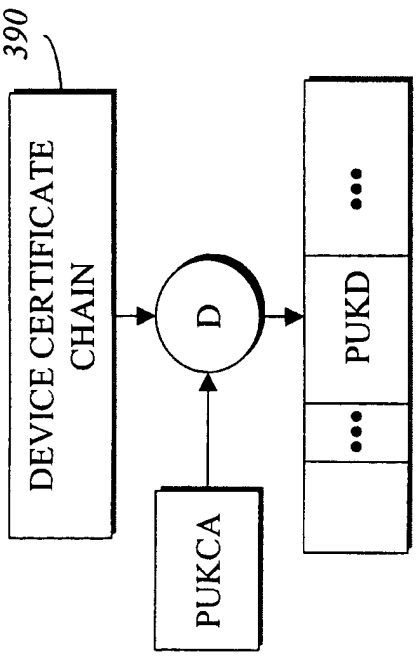


Figure 6

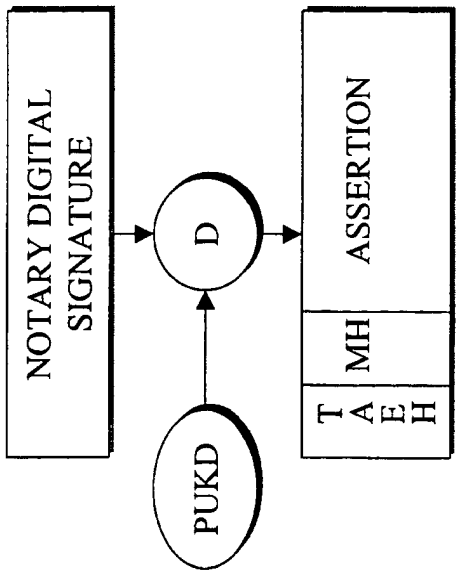


Figure 7

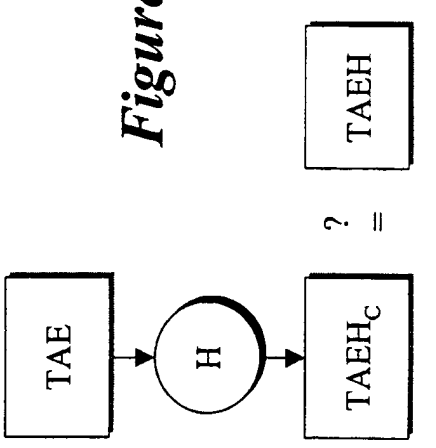


Figure 8

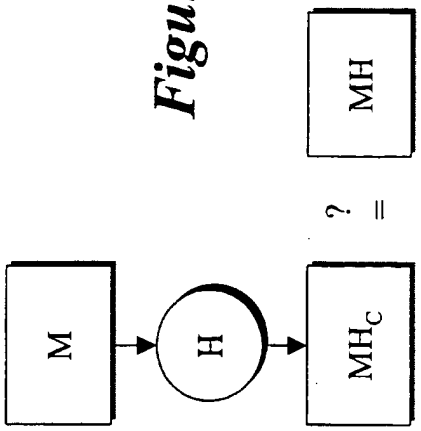


Figure 9

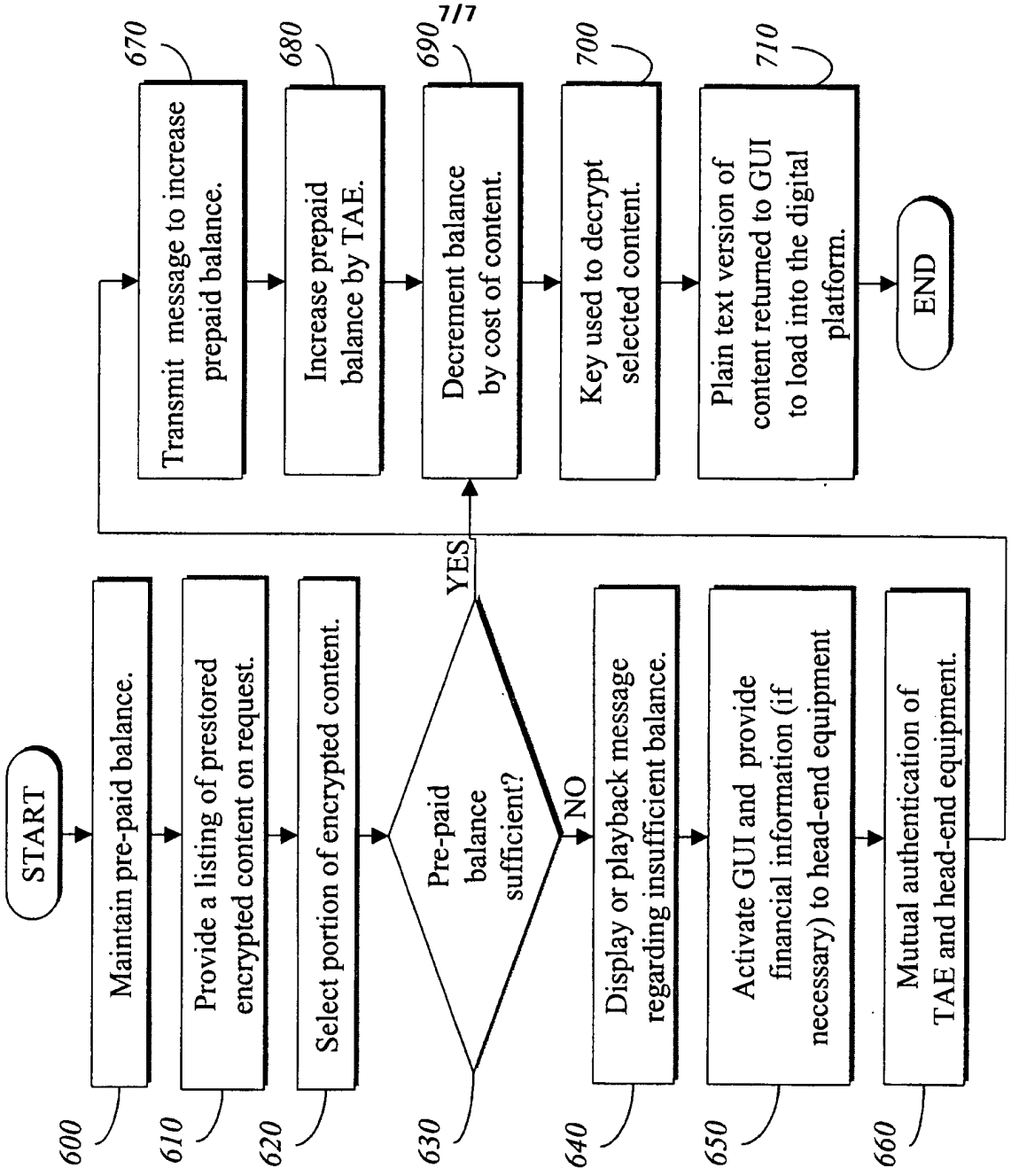

START
Maintain pre-paid balance.
Provide a listing of prestored encrypted content on request.
Select portion of encrypted content.
Pre-paid balance sufficient?
YES
NO
Display or playback message regarding insufficient balance.
Activate GUI and provide financial information (if necessary) to head-end equipment
Mutual authentication of TAE and head-end equipment.
Transmit message to increase prepaid balance.
Increase prepaid balance by TAE.
Decrement balance by cost of content.
Key used to decrypt selected content.
Plain text version of content returned to GUI to load into the digital platform.
END
600
610
620
630
640
650
660
670
680
690
700
710

Figure 10

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/08536

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 473 692 A (DAVIS DEREK L) 5 December 1995 (1995-12-05) abstract; figures 3-6 column 2, line 58 -column 4, line 22 column 5, line 47 -column 8, line 8	1-4
X	WO 98 45768 A (NORTHERN TELECOM LTD) 15 October 1998 (1998-10-15) the whole document	16,17
A		1,2,6-8, 11,14,15
Y	EP 0 778 512 A (SUN MICROSYSTEMS INC) 11 June 1997 (1997-06-11) abstract column 2, line 15 - line 43	20

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 July 2000	03/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/08536

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 235 642 A (WOBBER EDWARD ET AL) 10 August 1993 (1993-08-10) abstract; figures 2-4 column 1, line 30 - line 50	20
A		1,11,12, 20

A	US 5 892 904 A (ATKINSON ROBERT G ET AL) 6 April 1999 (1999-04-06) the whole document	2,6-8, 10,13, 14,17-19

A	EP 0 686 906 A (SUN MICROSYSTEMS INC) 13 December 1995 (1995-12-13)	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/US 00/08536

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5473692 A	05-12-1995	AU 3583295 A	27-03-1996
		EP 0780039 A	25-06-1997
		JP 10507324 T	14-07-1998
		WO 9608092 A	14-03-1996
		US 5568552 A	22-10-1996
WO 9845768 A	15-10-1998	AU 6492198 A	30-10-1998
		EP 0974084 A	26-01-2000
EP 0778512 A	11-06-1997	US 5708709 A	13-01-1998
		JP 9288575 A	04-11-1997
US 5235642 A	10-08-1993	EP 0580350 A	26-01-1994
		JP 6202998 A	22-07-1994
US 5892904 A	06-04-1999	NONE	
EP 0686906 A	13-12-1995	US 5724425 A	03-03-1998
		JP 8166879 A	25-06-1996